UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/852,562	05/10/2001	David M. Blaker	9269-4	6250

20792 7590 09/10/2004

MYERS BIGEL SIBLEY & SAJOVEC
PO BOX 37428
RALEIGH, NC 27627

EXAMINER	
NORRIS, TREMAYNE M	

ART UNIT	PAPER NUMBER
2137	

DATE MAILED: 09/10/2004

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	**Application No.** 09/852,562	**Applicant(s)** BLAKER ET AL.	
	Examiner Tremayne M. Norris	**Art Unit** 2137	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *10 May 2001*.

2a)□ This action is **FINAL**. 2b)☒ This action is non-final.

3)□ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-86* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)□ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-20,25-49,54-77 and 82-86* is/are rejected.

7)☒ Claim(s) *21-24,50-53 and 78-81* is/are objected to.

8)□ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)□ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *10 May 2001* is/are: a)☒ accepted or b)□ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)□ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)□ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)□ All b)□ Some * c)□ None of:

1.□ Certified copies of the priority documents have been received.

2.□ Certified copies of the priority documents have been received in Application No. _____.

3.□ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)

2) □ Notice of Draftsperson's Patent Drawing Review (PTO-948)

3) ☒ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08)
Paper No(s)/Mail Date *3/14/02; 4/5/02;*.

4) □ Interview Summary (PTO-413)
Paper No(s)/Mail Date. _____ .

5) □ Notice of Informal Patent Application (PTO-152)

6) □ Other: _____.

Claim Rejections - 35 USC § 102

1. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (b) the invention was patented or described in a printed publication in this or a foreign country or in public use or on sale in this country, more than one year prior to the date of application for patent in the United States.

2. Claims 1-3,30-32,59,60 rejected under 35 U.S.C. 102(b) as being anticipated by Welngart (EP 0560020).

Regarding claim 1, Welngart teaches a method of operating a cryptographic data processing system that comprises a host processors a system memory coupled to the host processor, and a cryptographic processor integrated circuit that comprises a local memory and is coupled to the host processor and the system memory, the method comprising:

loading at least one operand from the system memory to the local memory;

performing at least one operation on the at least one operand to generate a result in the local memory; and

storing the result generated in the local memory in the system memory (col.6 line 30 thru col.7 line 51).

Regarding claim 2, Welngart teaches performing the at least one operation, and storing the result are performed by the cryptographic processor without interaction with the host processor (col.6 line 30 thru col.7 line 51).

Regarding claim 3, Welngart teaches a cryptographic data processing system, comprising:

a host processor;

a system memory coupled to the host processor; and

a cryptographic processor that comprises a local memory and is coupled to the host processor and the system memory, the cryptographic processor being programmed to load at least one operand from the system memory to the local memory perform at least one operation on the at least one operand to generate a result in the local memory, and store the result generated in the local memory in the system memory (col.6 line 30 thru col.7 line 51).

Regarding claim 30, Welngart teaches a method of operating a data processing system that comprises a host processor, a system memory coupled to the host processor, and an adjunct processor integrated circuit that is coupled to the host processor and the system memory, the method comprising:

transferring information between the host processor and the adjunct processor using the system memory (col.6 line 30 thru col.7 line 51).

Claims 31 and 32 are substantially equivalent to claims 1 and 2 respectively, therefore claims 31 and 32 are rejected because of similar rationale.

Claims 59 and 60 are substantially equivalent to claims 1 and 2 respectively, therefore claims 59 and 60 are rejected because of similar rationale.

3. Claims 4-10,14,20,25-29,33-39,43,49,54-58,61-67,71,77,82-86 are rejected under 35 U.S.C. 102(b) as being anticipated by Hocevar et al (EP 0945788).

Regarding claim 4, Hocevar teaches a method of operating a cryptographic data processing system that comprises a host processor, a system memory coupled to the host processor, and a cryptographic processor integrated circuit that comprises a local memory and is coupled to the host processor and the system memory, the method comprising:

providing a command queue in the system memory;

loading a command block into the command queue using the host processor;

executing the command block using the cryptographic processor; and

notifying the host processor that the command block has been executed (col.3 line 38 thru col.4 line 38).

Regarding claim 5, Hocevar teaches providing a read address for the command queue and a write address for the command queue;

wherein loading the command block into the command queue using the host processor comprises loading the command block into the command queue using the host processor beginning at the write address, and wherein executing the command block using the cryptographic processor comprises executing the command block using the cryptographic processor beginning at the read address (col.4 line 39 thru col.5 line 21).

Regarding claim 6, Hocevar teaches loading the command block into the command queue using the host processor beginning at the write address comprises:

determining if the write address plus an amount corresponding to a size of a single command block equals the read address; and

loading the command block into the command queue using the host processor beginning at the write address if the write address plus the amount corresponding to the size of the single command block does not equal the read address (col.5 lines 14-21; col.6 lines 19-55).

Regarding claim 7, Hocevar teaches incrementing the write address by the amount corresponding to the size of a single command block using the host processor after loading the command block into the command queue using the host processor beginning at the writte address if the write address plus the amount corresponding to the size of the single command block does not equal the read address (col.5 lines 14-21; col.6 line 19 thru col.7 line 17).

Regarding claim 8, Hocevar teaches executing the command block using the cryptographic processor beginning at the read address comprises:

determining whether the read address is equal to the write address; and

executing the command block using the cryptographic processor beginning at the read address if the read address is not equal to the write address (col.5 lines 2-21).

Regarding claim 9, Hocevar teaches incrementing the read address by an amount corresponding to a size of a single command block using the cryptographic processor after executing the command block using the cryptographic processor beginning at the read address (col.5 lines 2-21; col.6 line 19 thru col.7 line 17).

Regarding claim 10, Hocevar teaches notifying the host processor that the command block has been executed comprises invoking an interrupt using the cryptographic processor after executing the command block (col.13 lines 16-33).

Regarding claim 14, Hocevar teaches loading at least one operand from the command queue to the local memory;

performing at least one operation on the at least one operand to generate a result in the local memory; and

storing the result generated in the local memory in the command queue (col.3 line 38 thru col.4 line 38).

Claim 20 is substantially equivalent to claim 4, therefore claim 20 is rejected because of similar rationale.

Regarding claim 25, Hocevar teaches a method of operating a cryptographic data processing system that comprises a host processor, a system memory coupled to the host processor, and a cryptographic processor integrated circuit that comprises a local memory and is coupled to the host processor and the system memory, the method comprising:

providing a command queue in the system memory;

providing a read address for the command queue and a write address for the command queue;

loading a random number sample into the command queue using the cryptographic processor beginning at the write address; and

reading the random number sample using the host processor beginning at the read address (col.3 line 38 thru col.5 line 21).

Regarding claim 26, Hocevar teaches loading the random number sample into the command queue using the cryptographic processor beginning at the write address comprises:

determining if the write address plus an amount corresponding to a size of a single random number sample equals the read address; and

loading the random number sample into the command queue using the cryptographic processor beginning at the write address if the write address plus the amount corresponding to the size of the single random number sample does not equal the read address (col.5 lines 14-21; col.6 lines 19-55).

Claims 27-29 are substantially equivalent to claims 7-9 respectively, therefore claims 27-29 are rejected because of similar rationale.

Claims 33-39 are substantially equivalent to claims 4-10 respectively, therefore claims 33-39 are rejected because of similar rationale.

Claim 43 is substantially equivalent to claim 14, therefore claim 43 is rejected because of similar rationale.

Claim 49 is substantially equivalent to claim 20, therefore claim 49 is rejected because of similar rationale.

Claims 54-58 are substantially equivalent to claims 25-29 respectively, therefore claims 54-58 are rejected because of similar rationale.

Claims 61-67 are substantially equivalent to claims 4-10 respectively, therefore claims 61-67 are rejected because of similar rationale.

Claim 71 is substantially equivalent to claim 14, therefore claim 71 is rejected because of similar rationale.

Claim 77 is substantially equivalent to claim 20, therefore claim 77 is rejected because of similar rationale.

Claims 82-86 are substantially equivalent to claims 25-29 respectively, therefore claims 82-86 are rejected because of similar rationale.

4. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

5. Claims 15,44,72 are rejected under 35 U.S.C. 102(e) as being anticipated by Hussain et al (US pat 6,075,546).

Regarding claim 15, Hussain teaches a method of operating a cryptographic data processing system that comprises a host processor, a system memory coupled to the host processor, and a cryptographic processor integrated circuit that is coupled to the host processor and the system memory, the method comprising:

providing a command queue in the system memory;

loading a command block into the command queue using the host processor;

setting a value of an interrupt field in the command block to request an interrupt when the command block has been executed;

executing the command block using the cryptographic processor', and

invoking an interrupt using the cryptographic processor after executing the command block if the interrupt field in the command block is set to the value to request the interrupt (col.2 lines 44-65; col.5 lines 10-25; col.6 line 59 thru col.7 line 6; col.8 lines 53-59).

Claim 44 is substantially equivalent to claim 15, therefore claim 44 is rejected because of similar rationale.

Claim 72 is substantially equivalent to claim 15, therefore claim 72 is rejected because of similar rationale.

Claim Rejections - 35 USC § 103

6. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

7. Claims 11-13, 17,18,40-42,46,47,68-70,74,75 are rejected under 35 U.S.C. 103(a) as being unpatentable over Hocevar, and further in view of Chi et al (US pat 5,706,489).

Regarding claim 11, Hocevar teaches the method of claim 4, but does not teach notifying the host processor that the command block has been executed comprises updating a completion field in the command block using the cryptographic processor. Chi teaches notifying the host processor that the command block has been executed comprises updating a completion field in the command block using the cryptographic processor (col.7 line 59 thru col.8 line 5; col.8 lines 42-50). It would have been obvious to one of ordinary skill in the art at the time of the invention to have combined Hocevar's data processing system with Chi's method of parallel instruction execution in order to enable database systems to expand accessed records asynchronously using inexpensive processors, thus greatly reducing the processing costs (Chi col.2 lines 16-32).

Regarding claim 12, Hocevar and Chi in combination teach the method as recited in claim 11, in addition Chi teaches providing a periodic interrupt; and

reading the completion field using the host processor upon invocation of the periodic interrupt (col.4 lines 48-55; col.8 lines 51-60; col.9 lines 55-57).

Regarding claim 13, Hocevar teaches the method of claim 4, but does not teach setting a timer after loading the command block into the command queue using the host processor; and checking whether the command block has been executed after expiration of the timer. Chi teaches setting a timer after loading the command block into the command queue using the host processor; and checking whether the command block has been executed after expiration of the timer (col.5 line 57 thru col.6 line 3). It would have been obvious to one of ordinary skill in the art at the time of the invention to have combined Hocevar's data processing system with Chi's method of parallel instruction execution in order to enable database systems to expand accessed records asynchronously using inexpensive processors, thus greatly reducing the processing costs (Chi col.2 lines 16-32).

Regarding claim 17, Hocevar teaches a method of operating a cryptographic data processing system that comprises a host processor, a system memory coupled to the host processor, and a cryptographic processor integrated circuit that is coupled to the host processor and the system memory, the method comprising:

providing a command queue in the system memory;

loading a command block into the command queue using the host processor,

executing the command block using the cryptographic processor (col.3 line 38 thru col.4 line 38).

What Chi teaches that Hocevar does not teach is updating a completion field in the command block using the cryptographic processor (col.7 line 59 thru col.8 line 5; col.8 lines 42-50). It would have been obvious to one of ordinary skill in the art at the time of the invention to have combined Hocevar's data processing system with Chi's method of parallel instruction execution in order to enable database systems to expand accessed records asynchronously using inexpensive processors, thus greatly reducing the processing costs (Chi col.2 lines 16-32).

Regarding claim 18, Hocevar and Chi in combination teach the method of claim 17, in addition Chi teaches providing a periodic interrupt; and reading the completion field using the host processor upon invocation of the periodic interrupt (col.4 lines 48-55; col.8 lines 51-60; col.9 lines 55-57).

Claims 40-42 are substantially equivalent to claims 11-13 respectively, therefore claims 40-42 are rejected because of similar rationale.

Claims 46 and 47 are substantially equivalent to claims 17 and 18 respectively, therefore claims 46 and 47 are rejected because of similar rationale.

Claims 68-70 are substantially equivalent to claims 11-13 respectively, therefore claims 68-70 are rejected because of similar rationale.

Claims 74 and 75 are substantially equivalent to claims 17 and 18 respectively, therefore claims 74 and 75 are rejected because of similar rationale.

8. Claims 16,45,73 are rejected under 35 U.S.C. 103(a) as being unpatentable over Hussain, and further in view of Lee et al (US pat 4,763,242).

Regarding claim 16, Hussain teaches the method of claim 15, but does not teach storing error information on the command block that is associated with executing the command block using the cryptographic processor. Lee teaches storing error information on the command block that is associated with executing the command block using the cryptographic processor (col.7 lines 1-23). It would have been obvious to one of ordinary skill in the art at the time of the invention to have combined Hussain's packetized command interface with Lee's system providing flexible processor extension in order to add hardware that extends a computer's processor capability without compromising software compatibility (Lee col.1 lines 9-21; col.2 lines 29-52).

Claim 45 is substantially equivalent to claim 16, therefore claim 45 is rejected because of similar rationale.

Claim 73 is substantially equivalent to claim 16, therefore claim 73 is rejected because of similar rationale.

9. Claims 19,48,76 are rejected under 35 U.S.C. 103(a) as being unpatentable over Hocevar and Chi as applied to claim17 above, and further in view of Lee.

Regarding claim 19, Hocevar and Chi in combination teach the method of claim 17, but do not teach storing error information on the command block that is associated with executing the command block using the cryptographic processor. Lee teaches storing error information on the command block that is associated with executing the command block using the cryptographic processor (col.7 lines 1-23). It would have been obvious to one of ordinary skill in the art at the time of the invention to have combined Hocevar and Chi's data processing system with Lee's system providing flexible processor extension in order to add hardware that extends a computer's processor capability without compromising software compatibility (Lee col.1 lines 9-21; col.2 lines 29-52).

Claim 48 is substantially equivalent to claim 19, therefore claim 48 is rejected because of similar rationale.

Claim 76 is substantially equivalent to claim 19, therefore claim 76 is rejected because of similar rationale.

Allowable Subject Matter

10. Claims 21-24, 50-53, and 78-81 are objected to as being dependent upon a rejected base claim, but would be allowable if rewritten in independent form including all of the limitations of the base claim and any intervening claims. The following is a statement of reasons for the indication of allowable subject matter:

With respect to claims 21,50, and 81, the cited prior art fails to specifically teach the data processing system comprises a cryptographic data processing system, the adjunct processor integrated circuit comprises a cryptographic processor integrated circuit, and performing the operation based on the input data comprises:

performing a hash operation based on the input data using the cryptographic processor to generate a hash value.

With respect to claims 22,51, and 79, the cited prior art fails to specifically teach storing the result in the input data field comprises:

storing the hash value in the input data field such that the at least a portion of the input data is overwritten.

With respect to claims 23,52, and 80, the cited prior art fails to specifically teach the command block further comprises an input pointer field that contains an address in the system memory of an incoming packet and wherein performing the hash operation comprises:

performing the hash operation based on the input data and the incoming packet using the cryptographic processor to generate the hash value.

With respect to claims 24,53, and 81 the cited prior art fails to specifically teach the command block further comprises an output pointer field that contains an address in the system memory for storing a decrypted packet, the method further comprising:

decrypting the incoming packet using the cryptographic processor to generate the decrypted packet;

attaching the hash value to the decrypted packet; and

storing the decrypted packet with the attached hash value at the address in the system memory contained in the output pointer field.

Conclusion

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Tremayne M. Norris whose telephone number is (571) 272-3874. The examiner can normally be reached on M-F 7:30AM-5:00PM alternate Fridays.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Andrew Caldwell can be reached on (571) 272-3868. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Tremayne Norris

September 5, 2004

Andrew Caldwell
Andrew Caldwell